



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

A

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,583	02/12/2002	Carl Young	G08.015	6976

28062 7590 11/29/2005

BUCKLEY, MASCHOFF, TALWALKAR LLC
5 ELM STREET
NEW CANAAN, CT 06840

EXAMINER

RAHMAN, FAHMIDA

ART UNIT PAPER NUMBER

2116

DATE MAILED: 11/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/074,583

Applicant(s)

YOUNG, CARL

Examiner

Fahmida Rahman

Art Unit

2116

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 12 February 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-28 are pending.

Information Disclosure Statement

2. The information disclosure statements filed on 11/20/03, 7/16/03 and 7/08/02 fail to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because the cited NPL literatures are not attached with the application.

The information disclosure statements have been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Oath/Declaration

3. A new oath or declaration is required because the pending application does not have any associated oath or declaration.

Art Unit: 2116

The new oath or declaration must properly identify the application of which it is to form a part, preferably by application number and filing date in the body of the oath or declaration. See MPEP §§ 602.01 and 602.02.

Specification

The disclosure is objected to because of the following informalities:

4. The words “complex associations and can be developed” cited in line 20 of page 6 of the specification should be corrected as: “complex associations can be developed”.
5. The words “this information is correlates with a low scaled weighting” cited in line 23 of page 6 of the specification should be corrected as: “this information is correlated with a low scaled weighting”.
6. Line 12 of page 6 of the specification refers “security level” with numeral 104. However, “security level” is referred with numeral 105 in Fig 1.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-21, 24, 25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Art Unit: 2116

Claims 1-21 disclose a computer implemented method for managing risk related to a security risk event, comprising receiving the information, structuring the information and calculating the security level. However, it is not appeared that the computer implemented method is limited to tangible embodiments, because the method is most likely a piece of software code without associated hardware.

Claim 24 discloses a program code resided on a computer readable medium. However, it is not appeared that the computer executable code is limited to tangible embodiments, because the code is a piece of software, which lacks tangibility.

Claim 25 discloses a computer data signal embodied in a digital data stream. However, it is not appeared that the computer data signal is limited to tangible embodiments, because the signal lacks tangibility.

Claim Objections

8. Claim 27 is objected to because of the following informalities:

claim 27 is dependent on claim 35, which is absent in the application. For the rest of the office action, it is assumed that claim 27 was intended to depend on claim 26. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 11-12 recite the limitation "the suggested security measure" in line 1.

There is insufficient antecedent basis for this limitation in the claim.

10. Claim 13 recite the limitation "the suggested action" in line 1. There is insufficient antecedent basis for this limitation in the claim.

11. Claims 22, 23, 26, 27 and 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 22 recites the limitation "a security risk event" in line 7. It is unclear whether it is intended to be the same or different from "a security risk event" recited in line 1. It is necessary to establish a relationship between the two recitations.

Claim 23 depends on claim 22. Thus, it carries the same ambiguities of claim 22.

Art Unit: 2116

Claim 26 recites the limitation “ a security management server” in lines 6-7. It is unclear whether it is intended to be the same or different from “a security management server” recited in line 3. It is necessary to establish a relationship between the two recitations.

Additionally, claim 26 recites the limitation “a security risk event” in lines 5, 6-7 and 8-9. It is unclear whether they are intended to be the same or different from each other. It is necessary to establish a relationship among all of the recitations of “a security risk event”.

Claims 27-28 depend on claim 26. Thus, they carry the same ambiguity of claim 26.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1-7, 10-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Teller-Kanzler et al (EP 0999489 A2).

For claim 1, Teller Kanzler et al teach **a computer-implemented method for managing risk related to a security risk event** (abstract 57), **the method comprising:**

Art Unit: 2116

- **receiving information relating to a security risk event** (s4 in Fig 6; lines 20-36 of column 3);
- **structuring the information received according to risk variables** (s5 in Fig 6; lines 54 of page 3 through line 10 of page 4); and
- **calculating a security level using the structured information and a set of relationships established between the risk variables** (lines 11-17 of column 4).

For claim 2, note line 15 of column 4, which mentions that the degree of business risk is assessed.

For claim 3, note 16 of Fig 1, which mentions organizational environment. Level 1 – level 5 of Fig 1 shows the degree of security level that the business facility can have. Thus, the security level comprises a security confidence level indicative of how secure a particular facility can be made relative to a particular security risk event.

For claim 4, note 18, 20 and 22 of Fig 2, Fig 3 and Fig 4, which mention security level in business commitment, policies, standards and security services. The 5 levels of 18, 20 and 22 can be indicative of how secure a particular practice can be made relative to a particular security risk event.

For claim 5, lines 12-20 of column 12 mention that the organization can graduate from

Art Unit: 2116

one level to next level when it reaches a certain score. Thus, security level comprises a security maintenance level indicative of a level of security that should be maintained in relation to an analyzed security risk event.

For claim 6, note lines 41-42 of column 2, which mention that the method develops a security infrastructure, which recommends solutions to deal with such threat. Thus, the method generates a suggested security measure according to the calculated security level and structured information.

For claim 7, note lines 29-41 of column 12, which mention that the score is used by business managers within the organization to make decision if they are satisfied with the particular level in light of the risk to the business of the organization. Therefore, the information received, the security stand of business and suggested security measures are stored for further consideration of business managers. Thus, the method comprises the step of: storing the information received, the security level and the suggested security measure.

For claim 10, note cell 11 of level 4 in Fig 3, which mentions that the determination of level of protection required for information assets is made. Thus, the suggested security measure comprises physical protection of media containing information relating to the transaction.

Art Unit: 2116

For claim 11, note the 5th cell of level 5 in Fig 4, which mention about full integration between physical security and information security. Thus, the suggested security measure comprises physical protection of a facility associated with the security risk.

For claim 12, cell 12 of level 5 in Fig 4 mentions about organization wide dissemination of security alerts, which is a physical protection of a building. Thus, the suggested security measure comprises physical protection of a building associated with a business transaction.

For claim 13, note cells 3 and 4 of level 5 in Fig 5, which mention that the help desk and organization wide reporting of security incidents. Thus, the suggested action comprises notifying an authority regarding potential breach of security.

For claim 14, lines 16-18 of column 12 mention that the score is used to determine if the organization can move from one level to next level. Thus, the score is an indicative of suggested security measure, which is a set of relationships between variables defined in ISEM grid.

For claim 15, note lines 24-27 of column 2, which mention that the information security infrastructure furnishes classifying the degree of risk associated with information asset. Thus, the level of analysis utilized in the calculation of the security level is rated according to a classification.

For claim 16, note lines 6-10 of column 4, which mention about the weighting of the categorized information security characteristics. Thus, the calculation comprises a level of weighting associated with a category of risk variables.

For claim 17, lines 12-25 of column 12 mention that the characteristics within a cell of ISEM grid is weighted according to it's importance and a score is computer. Thus, the calculation comprises aggregating multiple weightings of risk variables.

For claim 18, note line 22 of column 12, which mentions about the use of decision tree, a relationship algorithm. Thus, the calculation comprises a relationship algorithm that determines which variables effect other variables.

For claim 19, note line 22 of column 12, which mentions about the use of decision tree, a relationship algorithm. In addition, lines 12-16 of column 12 mention about the weighting of cells according to importance. The decision tree structure defines the relationship among variables, including the weighting. Thus, the calculation comprises a relationship algorithm that determines how first variable effect weighting of other variables.

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2116

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1, 6, 8-9, 22-28 are rejected under 102(e) as being anticipated by Townsend (US Patent Application Publication 2002/0188861).

For claim 1, Townsend teaches a computer implemented method for managing risk related to a security risk event (Fig 1), the method comprising:

- receive information relating to a security risk event (110 in Fig 1);
structure the information received according to risk variables (115 and 120);
- and calculate a security level (135) using the structured information and a set of relationships established between the risk variables (115, 120 and 130)

For claim 6, 145 provides the suggestion or recommendation.

For claim 8, 180 in Fig 1 shows the generation of diligence report.

For claim 9, Fig 6 shows the report, which comprises inquiries made ("no specific training identified") and security measures executed ("courses available")

For claims 22, Townsend teaches the following limitations:

A computerized system for managing risk related to a security risk event (Fig 1-7), the system comprising:

- **a computer server (730) accessible with a system access device (700, 724) via a communications network (726, 728, 722);**
- **and executable software stored on the server and executable on demand ([0061] of page 5), the software operative with the server to cause the system to:**
 - o **receiving information relating to a security risk event (Fig 2);**
 - o **structuring the information received according to risk variables (Fig 4); and**
 - o **calculating a security level using the structured information and a set of relationships established between the risk variables (130, 135 and 140 in Fig 1)**

For claim 23, the system of Townsend uses software to calculate security level. Thus, the software tool has to be feed with the information as shown in Fig 2 by an electronic means, since computer itself is an electronic device.

For claims 24 and 25, the system of Townsend must have the corresponding code and data signal to implement the system of claim 22.

Art Unit: 2116

For claim 26, Townsend teaches the following limitations:

A method of interacting with a network access device (Fig 7) so as to manage risk relating to a risk subject (Fig 1-6), the method comprising the steps of:

- **initiating interaction with a security risk management server (730) via a communications network (722, 726, 728);**
- **inputting information descriptive of a security risk event (Fig 2);**
- **transmitting the information descriptive of security risk event to a security risk management server (lines 1-5 of [0061] of page 5 mention that the server transmit the requested code for user to select strength level. Thus, the server receives appropriate information related to risk event);**
- **and receiving a security level calculated using the information descriptive of a security risk event and a set of relationships established between risk variables associated with the information descriptive of a security risk event (130 in Fig 1 shows the calculated level. [0061] of page 5 mention that the downloaded application allows a user to select the counter measure levels and the code may be executed by the processor as it is received. Thus, a security level is calculated and received by the system that uses the information relating to the risk event and the relationships among the risks variables)**

For claim 27, lines 10-13 of [0022] of page 2 mention that the application asset may comprise transaction system. Thus, the risk event can be a financial transaction.

Art Unit: 2116

For claim 28, [0061] of page 5 mentions about the selection of security measures by the user.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teller-Kanzler et al (EP 0999489 A2).

Teller-Kanzler et al do not teach recalculation of security explicitly.

However, lines 13-16 of column 14 of Teller-Kanzler et al mention that the various modifications would be apparent to ordinary skill in the art and the disclosure is intended to cover all such modifications.

One ordinary skill in the art would have been motivated to recalculate the security level responsive to new information and/or progression of chronology of events, since these events/information may make the change of score of the security level. In that case, management may feel that the existing level calculated by the method is not a proper

Art Unit: 2116

reflection of security model in light of new information or progressive chronology of events. They may want to verify that the new set of received information/progressive events still verifies the security level of the entity.

In addition, [0049] of column 12 mention that the managers use the score to determine whether they are satisfied with the level of organization in light of risk. Since, the new information or chronology of events may change the security level of the organization, recalculation is necessary to obtain the correct level of the organization in light of risk.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fahmida Rahman whose telephone number is 571-272-8159. The examiner can normally be reached on Monday through Friday 8:30 - 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lynne Browne can be reached on 571-272-3670. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2116

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Fahmida Rahman
Examiner
Art Unit 2116



LYNNE H. BROWNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100